IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

DECLARATION OF ANDREW W. APPEL
IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION

ANDREW W. APPEL, declares, under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

1. My name is Andrew W. Appel.

2. My background, qualifications, and professional affiliations are set forth in my curriculum vitae, which is attached as Exhibit A. I have over 40 years' experience in computer science, and 15 years' experience studying voting machines and elections.

3. I am the Eugene Higgins Professor of Computer Science at Princeton University, where I have been on the faculty since 1986 and served as Department Chair from 2009-2015. I have also served as Director of Undergraduate Studies, Director of Graduate Studies, and Associate Chair in that department. I have

served as Editor in Chief of ACM Transactions on Programming Languages and Systems, the leading journal in my field. In 1998 I was elected a Fellow of the Association for Computing Machinery, the leading scientific and professional society in Computer Science.

4. I received an A.B. (1981) from Princeton University *summa cum laude* in Physics, and a PhD (1985) from Carnegie Mellon University in Computer Science.

5. I have taught undergraduate and graduate courses at Princeton University in programming, programming languages, software engineering, election machinery, software verification, and formal methods.

6. I have testified on election technology before the U.S. House of Representatives (subcommittee on information technology, 2016), the New Jersey legislature (several committees, on several occasions 2005-2018), the Superior Court of New Jersey (Mercer County, 2009; Cumberland County, 2011), the New York State Board of Elections (2019), the Freeholders of Mercer County (2017 and 2019) and Essex County (2019).

7. I have published over 100 scientific articles and books, including many papers on computer security and several papers on voting machines, election technology, and election audits.

8. I have served as a peer-review referee for the Usenix Electronic Voting Technology workshop.

9. I am not being compensated for my work related to this matter. I expect that my expenses, if any, will be reimbursed.

III. Dr. Shamos is incorrect regarding paper ballot risks.

10. I have read the Declaration of Michael Shamos, Ph.D., J.D., Doc. No. 472-1 filed July 10, 2019 in the above-captioned matter.

11. In general, Dr. Shamos's arguments against paper ballots are either irrelevant to current technology or to Curling Plaintiffs' proposed relief, or they apply equally to systems already in use by Georgia.

12. In paragraph 36, Dr. Shamos writes, "the paper ballot is the only record of the voter's choices." This is untrue, especially in precinct-count optical scan (PCOS) voting—which I understand is the method of voting proposed in the relief requested by Curling Plaintiffs. Generally in PCOS voting, the voter feeds his or her ballot directly into the PCOS machine, which electronically scans it and records the vote choices (and modern PCOS machines also scan a high-resolution image of the entire page). Yes, the PCOS is a computer that can be hacked, and therefore the paper ballot marked by the voter should be the *presumptive* record of the vote, but the memory image in the PCOS can provide important forensic evidence if it is suspected that the paper ballots have been tampered with. In this way, the electronic record inside the PCOS (and also in the results cartridge

removed from the PCOS at the close of the election day) serve the same role they do in the DREs that Dr. Shamos discusses in his paragraph 37.

13. In paragraph 37, Dr. Shamos allows that memory cards of DREs can be tampered with, but claims that "such a manipulation does not change the redundant records that are retained on each individual voting machines, and does not change the paper tabulations that are produced at the close of polls in each individual polling place and signed by election judges. … Any discrepancy would be investigated …." He continues in paragraph 38, "if there is a discrepancy between optical scan totals and hand-counting, the hand-counted totals are always used in the naïve belief that they are more reliable…."

14. It is not clear to me why Dr. Shamos believes that discrepancies with DREs would be investigated, but with PCOS machines the election officials or the courts would be too naïve to investigate. Dr. Shamos cites nothing to support this conclusion, nor does this conclusion follow from common sense.

15. In paragraph 43, Dr. Shamos shows a large figure showing approximately 18 steps in the chain of custody of paper ballots in Los Angeles County. He neglects to mention that almost exactly the same 18 steps are required for the chain of custody of electronic vote cartridges produced by DRE machines.

16. In paragraph 44, Dr. Shamos alleges that "ballot boxes are completely out of view of the public or poll watchers for a substantial period of time" and

volunteers a hypothetical scenario in which a "political operative bribes an insider to stop off while transporting ballot boxes to a tabulation center" and replaces the actual ballots with "pre-prepared ballots marked to favor his party's candidates." These allegations completely ignore that Georgia rules provide for public setup, testing, tabulation, and consolidation of votes, and no laws nor practical hurdles prevent the public or poll-watchers from tracking the ballot boxes from the precincts to be tabulated.[1]

17. Dr. Shamos's claim that "[i]n every election cycle in the United States, ballot boxes are found weeks after the election in place (such as lakes and rivers) making it clear that they were never counted" (¶ 39) is also inaccurate and misleading.

a. The first citation he offers (¶ 39 n.4) shows that, in fact, the optical scanners made a complete count of the ballots that were only later left behind. Moreover, while the chain of custody for a single box of ballots may have been broken, the ballots were not lost, thereby preserving the ability to check the paper records against the electronic optical scan records.

b. Another citation Dr. Shamos offers (¶ 39 n.7) is irrelevant to in-precinct ballot boxes, which I understand is the relief advocated by Curling

[1] *See* O.C.G.A. §§ 21-2-379.11(f), 21-2-408; Ga. Comp. R. & Regs. 183-1-12-.02(5)(a)(8), (c)(4).

Plaintiffs here. Rather, this citation is about ballot drop-boxes (used in some states as an alternative to returning absentee ballots by mail), which are not used in Georgia nor are they part of the Curling Plaintiffs' proposed relief. The security measures, access, and timing surrounding those drop-boxes are different and not comparable to the procedures in place for in-precinct voting.[2]

c. Dr. Shamos's citation regarding Broward County (¶ 39 n.9) demonstrates that a careful recanvas better accounts for all ballots—consistent with the goal of the relief sought by Curling Plaintiffs.

d. Dr. Shamos cites fraud with paper absentee ballots in North Carolina (¶ 39 n.10, and again in ¶ 41) – but Georgia already employs paper absentee ballots. Presumably Dr. Shamos is not suggesting that this evidence is indicative of what happens in Georgia, in which case it would be a critical, ongoing problem in Georgia unrelated to Curling Plaintiffs' proposed relief.

18. In his paragraphs 55 and 56, Dr. Shamos implies that because optical scanners may interpret ballots differently than humans would during a recount, therefore some sort of problem ensues. But then in the first sentence of paragraph

[2] See, e.g., https://govt.westlaw.com/calregs/Document/I118620FA785243678FC16FA7D8FF09BD?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Default).

57, he says that in these cases a manual recount would get the true result intended by the voter. Exactly! This very point undermines Dr. Shamos's overall conclusions, and supports Curling Plaintiffs' proposed relief. Audits or recounts of papers ballots can correct for fraudulent hacking of voting machines *and* can correct for accidental miscalibration or misconfiguration of voting machines.

19. In paragraph 56, Dr. Shamos discusses optical-scan voting machines, but refers to an obsolete technology that has not been manufactured in the U.S. for over a decade. He refers to "each optical scan sensor (and there is one for each column of the ballot)." Such voting machines were made in the 20th century, but 21st-century optical-scan voting machines take a high-resolution digital scan of the ballot page and then use algorithms to interpret the voter's marks. Perhaps Dr. Shamos has not studied the last two generations of optical-scan voting machines certified by the E.A.C.

IV. Dr. Shamos's conclusions regarding DREs are incorrect

20. Contrary to Dr. Shamos's conclusions, Dr. Halderman's description of how DREs can be easily hacked is consistent with the scientific consensus, as described in peer-reviewed academic publications and in other venues, and agrees with my own research and study of this issue. Dr. Shamos's claims (of the supposed difficulty in hacking) in his paragraphs 87-90 and 92-95 are incorrect, unsupported

by scientific research, contradicted by the published scientific research, and inconsistent with the scientific consensus.

21. It is well understood by computer scientists that computers (since 1950) are "stored program" machines, that is, the program that determines how they compute is stored in the memory of the computer itself. Replacing this program with a different program will instruct the computer in a different way. Replacing a legitimate vote-counting program in a DRE with a different program that fraudulently miscounts the votes will instruct the computer to fraudulently miscount the votes. Installation of a fraudulent program can be done in the factory before the DRE is shipped, it can be done by anyone with physical access to the machine, and it can be done in other ways.

22. A DRE can be "hacked," that is, its computer program in memory can be replaced by a fraudulent program, by an attacker who never even comes within 100 miles of the machine. Before every election, election workers must install "ballot definition cartridges" into each voting machine. These cartridges are programmed in the election-management computers of a state or of a county, or by a private contractor. The *same* cartridges and the *same* physical insertion method is used to install new vote-counting programs into the DRE; this provision was designed (by

the manufacturer) to support the "firmware upgrade" process, whereby voting machines can be "upgraded" in the field[3].

23. An attacker who can hack into the election-management system can "hijack" the (otherwise legitimate) ballot-definition-insertion process and turn it into an (illegitimate) firmware-upgrade process. This method is documented in the scientific literature[4] [5] [6], and has been demonstrated in the laboratory.

24. Election-management computers must be routinely (directly or indirectly) connected to the internet (or to the phone system, which nowadays is the same thing) for a variety of purposes, including the dissemination of election results.

25. It is well-known (and documented) as a matter of science, and to anyone who reads the newspaper, that computer systems connected (directly or indirectly) to the internet are often hacked, that is, infiltrated by malicious attackers. Computers have been hacked that are owned and managed by businesses (including large and small retailers, insurance companies, phone companies, and internet companies) and governments (including the U.S. government, state governments, and municipalities).

---

[3] This sentence characterizes most but not all DRE voting machines, and characterizes the DREs used in Georgia.
[4] Security Analysis of the Diebold AccuVote-TS Voting Machine, by Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, *Proc. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '07),* August 2007
[5] Security evaluation of ES&S voting machines and election management system., by Aviv, A., Černy, P., Clark, S., Cronin, E., Shah, G., Sherr, M., & Blaze, M. *Proceedings of the conference on Electronic voting technology,* p. 11, July 2008.
[6] The New Jersey Voting-machine Lawsuit and the AVC Advantage DRE Voting Machine, by Andrew W. Appel, Maia Ginsburg, Harri Hursti, Brian W. Kernighan, Christopher D. Richards, Gang Tan, and Penny Venetis. *EVT/WOTE'09, Electronic Voting Technology Workshop / Workshop on Trustworthy Elections*, August 2009.

26. In cases where the hacker has wished to be stealthy, in some cases the hacks have survived for many years without detection.[7] [8]

27. Therefore Dr. Shamos is incorrect in asserting that it would be impractical to hack Georgia's DREs by a fully remote attack, and that any such attack would be readily detected.

28. In paragraph 89, Dr. Shamos says, "the machines' software is tested by independent testing authorities." Such testing is irrelevant. That testing was performed once, long ago, on a few instances of the DREs. It is not performed on the DREs in the field, and therefore could not possibly detect any fraudulent software installed in those DREs.

29. Dr. Shamos, in his paragraphs 97-101, promotes and defends "parallel testing." Parallel testing would be an extremely labor-intensive and impractical means of detecting DRE fraud, if it were ever done as thoroughly as would be necessary to be reliable. There is no evidence that parallel testing has ever been done, in any state, at a large enough scale to reliably assure the absence of DRE hacking.

[7] Inside the West's failed fight against China's 'Cloud Hopper' hackers, By Jack Stubbs, Joseph Menn, and Christopher Bing, Reuters News Service, June 26, 2019.
[8] Hackers are stealing years of call records from hacked cell networks, by Zack Whittaker, techcrunch.com, June 24, 2019.

30. Chris Harvey, Director of Elections of the State of Georgia, in a letter[9] dated August 1, 2018 to County Commissioners, describes an extremely ad-hoc and lightweight regime of parallel testing used by Georgia in 2018. Based on this description, I can say that Georgia does not do effective parallel testing of DREs.

V. Dr. Shamos's claims go against the weight of scientific consensus

31. In 2017 I was appointed by the National Academies of Science, Engineering, and Medicine (NASEM) to serve on a Consensus Study Committee on the Future of Voting. I served on that study committee, which comprised five computer scientists, one mathematician, two political scientists, one law professor, three election officials (from Wisconsin, Texas, and California), and was chaired by two university presidents (one a computer scientist by background, the other a law professor).

32. This NASEM study committee met for five two-day meetings over 16 months, heard testimony from many experts and election administrators, and drafted a comprehensive report in June 2018. This report was sent by NASEM for thorough peer review by a panel of 14 expert reviewers, overseen by a computer-science professor and a law professor who were independent of the study group.

[9] http://www.accg.org/docs/policy/8-1-18%20Letter%20from%20Chris%20Harvey%20to%20County%20Commissions.pdf

After it passed peer review, it was released by NASEM in September 2018, with the title *Securing the Vote: Protecting American Democracy.*

33. The NASEM consensus study report makes many specific recommendations, backed up by lengthy scientific justification. Two of our key recommendations are:

> *4.11. Elections should be conducted with human-readable paper ballots. These may be marked by hand or by machine (using a ballot-marking device); they may be counted by hand or by machine (using an optical scanner). Recounts and audits should be conducted by human inspection of the human-readable portion of the paper ballots. Voting machines that do not provide the capacity for independent auditing (e.g., machines that do not produce a voter-verifiable paper audit trail) should be removed from service as soon as possible.*
>
> *4.12. Every effort should be made to use human-readable paper ballots in the 2018 federal election. All local, state, and federal elections should be conducted using human-readable paper ballots by the 2020 presidential election.*

34. Our report represents the true scientific consensus not only of the committee itself, but also (to the best of our ability) of the broader scientific community; and this consensus was also tested by the external peer reviewers, who would not have let non-consensus recommendations pass unchallenged.

35. In general (and specifically on these recommendations 4.11 and 4.12) the committee did not have difficulty reaching consensus or identifying the broad scientific consensus; the science here is clear.

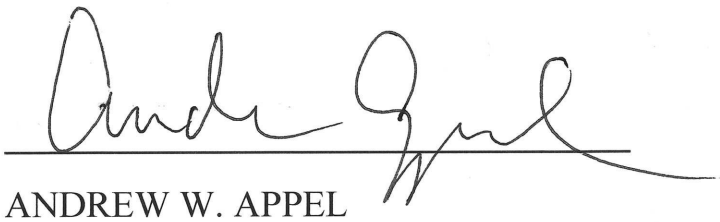
36. Those members of our committee who are computer scientists have substantial expertise in computer security with applications to elections, and at least three have studies issues specifically pertaining to paper ballots and to the security of voting machines such as DREs and optical scanners. Those members of our committee who were state-level or county-level election officials have many years of experience administering elections with voting machines and paper ballots.

37. I have been studying voting machines, as a substantial part of my scientific work, since 2004. I have taught two courses on "Election Machinery" at Princeton University. I have written papers on the security analysis of DRE voting machines, on security seals for voting machines, on election auditing, on internet voting, on ballot-marking devices. I have also written 58 short articles (between 2008 and 2019) about voting machines and elections, on Princeton University's "Freedom to Tinker: research and expert commentary on digital technologies in public life."

38. During the period 2004-19 I have spoken with, or corresponded with, or read the work of, well over 100 experts on the computer science of voting machines. In preparing this declaration, I also reviewed the scientific literature since 2007 on voting machines, with publications by dozens of scientists. On these bases, I understand that, with one exception, all computer-science experts on voting machines recognize that voting machines are not difficult to reprogram (to

"hack" if reprogrammed without authorization) and therefore it is unacceptably insecure to use paperless DRE voting machines in public elections. The sole exception I have identified across my extensive experience and research in the field is Michael I. Shamos: he is the sole computer scientist whom I have identified who purports to believe that DREs are acceptably insecure.[10] He is an outlier to the scientific consensus.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 17th day of July, 2019 in Princeton, New Jersey.



ANDREW W. APPEL

[10] Dr. Merle S. King, formerly a Professor at Kennesaw State University in Georgia, is also a computer scientist who has defended DREs. In 2004 he published one paper endorsing the use of DREs in Georgia. I cannot find any other scientific articles he has written. Implementing Voting Systems: the Georgia Method, by Brit J. Williams, Merle S. King. Communications of the ACM, October 2004, Vol. 47 No. 10, Pages 39-42.